GUIDELINES ON PERSONAL DATA BREACH NOTIFICATION - STRESS TEST ON RISK GOVERNANCE

The General Data Protection Regulation (the GDPR) provides for mandatory breach notification and communication requirements. The GDPR will apply from 25 May 2018. Non-compliance may expose organisations to penalties ranging up to EUR 10 million or 2% of global turnover, claims for damages and may affect reputation. The revised guidelines on Personal data breach notification[1] set actions to comply with the GDPR.

Key issues

- Mandatory notification of personal data breach within 72 hours.
- Mandatory information to individuals.
- Fines up to 2% of global annual turnover for failure to notify or inform individuals.
- Personal data breaches treated as security and cyber security incidents.
- Prompt awareness of any personal data breach alert.
- Lead supervisory authority for EU cross-border breaches.
- Additional notification obligations upon electronic trust service providers and operators of essential and digital services under eIDAS Regulation and NIS Directive.

THE PERSONAL DATA BREACH NOTIFICATION AND COMMUNICATION UNDER THE GDPR

The **data controller** (the organisation deciding on the purpose and means of the personal data processing) must (i) notify a **personal data breach** to the supervisory authority within 72 hours after becoming "**aware"** of it and (ii) **communicate** the personal data breach to the data subject without undue delay.

The GDPR has also introduced the obligation upon a **data processor** (i.e., a third party service provider that processes personal data on behalf of the controller customer) to notify the controller **without undue delay** after becoming "aware" of a personal data breach. **Legal responsibility to notify the supervisory authority continues to rest with the controller**.

Controllers should i**mmediately establish that personal data breaches have occurred** and act to avoid or contain their effects through appropriate technical protection measures such as:

- encrypting personal data;
- ensuring that processing systems (*e.g.* data storage tools) are resilient;
- timely restoring availability and access to personal data after incidents;
- regularly testing the security system adopted.

Personal data breach

Personal data breach is basically a **security incident,** which may fall in the following categories according to the Guidelines:

[1] The guidelines have been adopted by the Article 29 Working Party, composed, among others, of representatives of the supervisory authorities of each EU Member State (the Guidelines). This working party has advisory status and acts independently.

- "**Confidentiality breach**", in case of unauthorised or accidental disclosure of personal data or unauthorised access to such data;
- "**Integrity breach**", in case of unauthorised or accidental alteration of personal data;
- "**Availability breach**", in case of accidental or unauthorised loss of access to personal data or destruction of such data.

Examples: according to the Guidelines, the loss of a **decryption key** to access encrypted personal data is an availability breach, when the controller cannot restore access to the data. The controller must therefore notify the supervisory authority.

Temporary loss of availability for an **infection by ransomware** could lead to unauthorised access to personal data and then result in a confidentiality breach (and not in an "availability breach", provided that the access to data can be restored). The controller must therefore notify the supervisory authority.

"Becoming aware" of a personal data breach

According to the Guidelines, the controller becomes "aware" of a personal data breach when it has a **reasonable degree of certainty** that a security incident compromising personal data has occurred.

The controller has the obligation to ensure that it will be **immediately "aware"** of personal data breaches, so as to be able to take prompt action.

Assessing when a controller becomes "aware" of a breach must be analysed on a case-by-case basis.

Example: if a USB key with **unencrypted** personal data is lost, according to the Guidelines the controller becomes "aware" of this personal data breach **when it learns the key is lost**. The controller is "aware" of the personal data breach even though it cannot assess whether (or not) unauthorised people have gained access to the personal data.

To improve the chance to become "aware" in a timely manner and to ensure appropriate actions to contain a personal data breach, organisations could in advance determine **who has operational responsibility** within the organisation for managing personal data breaches.

Not having all necessary information on the personal data breach does not exempt the controller from its obligation to notify. This is likely to happen in more complex breaches, such as **cyber security incidents**, where investigations may be necessary to establish the nature and the extent of the breach. In this event, the controller informs the supervisory authority that it will immediately provide the required information as it becomes available.

Risk to the rights and freedoms of natural persons

Risk to the rights and freedoms of individuals is a key trigger requiring notification to the supervisory authority and communication to the data subject, provided that:

- breaches "unlikely to result in a risk to the rights and freedoms of natural persons" do not require notification to the supervisory authority under the GDPR, according to the guidelines; and

- controllers must communicate the personal data breach to the data subject when the personal breach is likely to result in a **high risk to the rights and freedoms** of the natural persons concerned. **A high risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached**.

  Examples: discrimination, identity theft or fraud, financial loss or damage to reputation. Disclosure of data revealing racial or ethnic origin, political opinion, sexual habits, religion or genetic data is also likely to damage individuals.

Controllers should, therefore, assess the risk resulting from a personal data breach immediately after becoming "aware" of it. This will also help the controller to take **effective steps** to contain the personal data breach.

EU cross-border breaches

The controller must notify a cross-border breach to the so-called **lead supervisory authority**, *i.e.* the authority of the Member State where the controller has its main or single establishment. This is not necessarily the authority of the Member State where the affected data subjects are located, or where the personal data breach occurred.

Non-EU data controllers

The GDPR catches operators with no base in the European Union when they target offers of goods or services to, or monitor the behaviour of, individuals in the EU. These operators must designate a representative in the European Union and **notify** personal data breaches to the **supervisory authority** of the EU Member State where the representative is established.

Notification obligations under eIDAS Regulation and NIS Directive

In addition to the notification and communication obligations under the GDPR, further notification obligations may apply, in accordance with:

- the **eIDAS Regulation** (no. 910/2014). Pursuant to this Regulation, an electronic trust service provider (the provider of certificates to create and validate electronic signatures and to authenticate signatories) must notify its supervisory body of breaches of security or loss of integrity with significant impact on the trust service provided or on the personal data maintained through the trust service.
- the **NIS Directive** (no. 1148/2016). Under this Directive, operators of essential services (providers of services with remarkable impact over social community, such as services in the banking, energy, transport and health sectors) and digital service providers (providers of on-line services such as e-commerce, on-line search engines and cloud services) must notify security incidents to their supervisory authority.

The NIS Directive provides for a general obligation upon the operators of essential services to implement technical and organisational measures to handle the risks posed to the security of the network and information system. The NIS Directive must be enforced by EU member States by 9 May 2018.

CONTACTS

KEY CONTACTS FOR THIS BRIEFING

Carlo Felice Giampaolino
Partner

T +39 064229 1356
E carlofelice.giampaolino@cliffordchance.com

Alessandro Sciarra
Associate

T +39 064229 1384
E alessandro.sciarra@cliffordchance.com

OUR DATA PRIVACY EXPERTS

UK

Jonathan Kewley
Partner

T +44 20 7006 3629
E jonathan.kewley@cliffordchance.com

Samantha Ward
Senior Associate

T +44 207006 8546
E samantha.ward@cliffordchance.com

US

Megan Gordon
Partner

T +1 202912 5021
E megan.gordon@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver@cliffordchance.com

Alice Kane
Counsel

T +1 212 878 8110
E alice.kane@cliffordchance.com

www.cliffordchance.com

Clifford Chance, Piazzetta M.Bossi, 3, 20121 Milan, Italy

Clifford Chance Studio Legale Associato

Abu Dhabi • Amsterdam • Bangkok • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.